LINEA NETWORK
PROFESSIONAL

Atlantis



Wireless N 300Mbps MultiFunction Access Point

Manuale

NetFly AP3 WN

ITALIANO

Questo prodotto è coperto da garanzia Atlantis della durata di 2 anni. Per maggiori dettagli in merito o per accedere alla documentazione completa in Italiano fare riferimento al sito **www.atlantis-land.com.**

ENGLISH

This product is covered by Atlantis 2 years warranty. For more detailed informations please refer to the web site **www.atlantis-land.com.**

For more detailed instructions on configuring and using this device, please refer to the online manual.

FRANCAIS

Ce produit est couvert par une garantie Atlantis de 2 ans. Pour des informations plus détaillées, référez-vous svp au site Web **www.atlantis-land.com.**

DEUTSCH

Dieses Produkt ist durch die Atlantis 2 Jahre Garantie gedeckt. Für weitere Informationen, beziehen Sie sich bitte auf Web Site **www.atlantis-land.com.**

ESPAÑOL

Este producto esta cubierto por Atlantis con una garantía de 2 años. Para mayor información diríjase a nuestro sitio Web **www.atlantis-land.com.**

INDICE

APPENDICE

A02-AP3-W300N_MI01 (v1.00 Aprile 2010)

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

Restrizioni di responsabilità CE/EMC

Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.

Se il prodotto fosse utilizzato con un PC/apparati non certificati, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l'utilizzatore è responsabile della "compliance" con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.

CE Mark Warning

In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

Dichiarazione di Conformità

Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo

riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-1, EN 301 489-17(compatibilità elettromagnetica) ed EN 60950 (sicurezza 2006/95/EC). Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:

Francia(FR): Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per infor mazioni ulteriori consultare *www.art-telecom.fr*.

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestichi genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.

Italia(IT): Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: *www.comunicazioni.it*.

Lussemburgo: Se utilizzato per servizi network o privati è da richiedere l'autorizzazione.
Norvegia (NO): apparecchiatura da non utilizzare in un aresa geografica di 20 km di raggio nei pressi di Ny Alesund.
Russia (CCP): solo per uso interno.

Dichiarazione di Conformità Sintetica

Con la presente dichiariamo che questo apparato è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttive 1999/5/CE. La dichiarazione di conformità nella sua forma completa è disponibile presso il sito www.atlantis-land.com (alla pagina del prodotto) o può essere richiesta a info@atlantis-land.com.



Importanti informazioni per il corretto riciclaggio/smaltimento di questa apparecchiatura

Il simbolo qui sotto indicato, riportato sull'apparecchiatura elettronica da Lei acquistata e/o sulla sua confezione, indica che questa apparecchiatura elettronica non potrà essere smaltita come un rifiuto qualunque ma dovrà essere oggetto di raccolta separata.
Infatti i rifiuti di apparecchiatura elettroniche ed elettroniche devono essere sottoposti ad uno specifico trattamento, indispensabile per evitare la dispersione degli inquinanti contenuti all''interno delle apparecchiature stesse, a tutela dell'ambiente e della salute umana. Inoltre sarà possibile riutilizzare/riciclare parte dei materiali di cui i rifiuti di apparecchiature elettriche ed elettroniche sono composti, riducendo così l'utilizzo di risorse naturali nonché la quantità di rifiuti da smaltire.
Atlantis, in qualità di produttore di questa apparecchiatura, è impegnato nel finanziamento e nella gestione di attività di trattamento e recupero dei rifiuti di apparecchiature elettriche ed elettroniche compatibili con l'ambiente e con la salute umana.
E' Sua responsabilità, come utilizzatore di questa apparecchiatura elettronica, provvedere al conferimento della stessa al centro di raccolta di rifiuti di apparecchiature elettriche ed elettroniche predisposto dal Suo Comune. Per maggiori informazioni sul centro di raccolta a Lei più vicino, La invitiamo a contattare i competenti uffici del Suo Comune.
Qualora invece avesse deciso di acquistare una nuova apparecchiata elettronica di tipo equivalente e destinata a svolgere le stesse funzioni di quella da smaltire, potrà portare la vecchia apparecchiatura al distributore presso cui acquista la nuova. Il distributore sarà tenuto ritirare gratuitamente la vecchia apparecchiatura[1].
Si tenga presente che l'abbandono ed il deposito incontrollato di rifiuti sono puniti con sanzione amministrativa pecuniaria da € 103 a € 619, salvo che il fatto costituisca più grave reato. Se l'abbandono riguarda rifiuti non pericolosi od ingombranti si applica la sanzione amministrativa pecuniaria da € 25 a € 154.

Il suo contributo nella raccolta differenziata dei rifiuti di apparecchiature elettriche ed elettroniche è essenziale per il raggiungimento di tutela della salute umana connessi al corretto smaltimento e recupero delle apparecchiature stesse.

1 Il distributore non sarà tenuto a ritirare l'apparecchiatura elettronica qualora vi sia un rischio di contaminazione del personale incaricati o qualora risulti evidente che l'apparecchiatura in questione non contiene i suoi componenti essenziali o contiene rifiuti diversi da apparecchiature elettriche e/o elettroniche.

NB: le informazioni sopra riportate sono redatte in conformità alla Direttiva 2002/96/CE ed al D. Lgs. 22 luglio 2005, n.[·] che prevedono l'obbligatorietà di un sistema di raccolta differenziata nonché particolari modalità di trattamento e smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE). Per ulteriori informazioni in materia, la invitiamo a consultare il nostro sito www.atlantis-land.com

AVVERTENZE

- Lasciare almeno 30cm di distanza tra l'antenna del dispositivo e l'utilizzatore.
- Non usare il dispositivo in un luogo in cui ci siano condizioni di alte temperatura ed umidità, il dispositivo potrebbe funzionare in maniera impropria e danneggiarsi.
- Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del dispositivo in oggetto
- Non aprire in nessun caso il case del dispositivo. Questa operazione è molto rischiosa per la presenza di voltaggio elevato. Ogni tentativo di apertura del dispositivo, inoltre, invalida la garanzia dello stesso.
- Se il dispositivo dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.
- Non effettuare upgrade del firmare utilizzando apparati/client wireless ma solo wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.
- Scollegare il dispositivo dalla presa elettrica prima di purirlo. Non utilizzare alcun tipo di solvente liquido o in spray. Utilizzare un panno soffice asciutto.

La garanzia del prodotto è invalidata nei seguenti casi : fulmini, errato voltaggio e sovratensioni violente in ingresso.

Forti urti o vibrazioni potrebbero danneggiare il dispositivo ed annullare così la garanzia.

Il throughput reale minimo è funzione di differenti fattori (non ultimo la distanza reale) e pertanto risulta non garantibile a priori.

Tutte le condizioni di utilizzo, avvertenze e clausole contenute in questo manuale e nella garanzia si intendono note ed accettate. Si prega di restituire immediatamente (entro 7 giorni dall'acquisto) il prodotto qualora queste non siano accettate.

Atlantis invita a visitare il sito web www.atlantis-land.com alla relativa pagina di prodotto per reperire manualistica e contenuti tecnici (aggiornamenti driver e/o funzionalità, utility, support note) aggiornati.

La ringraziamo per aver scelto un prodotto Atlantis. Questa manuale fornisce una panoramica per una rapida installazione del prodotto (nella prima parte), mentre la seconda parte illustra tutti i dettagli per una configurazione completa dell'apparato.

1. Introduzione

Acess Point Multi-Funzione in standard IEEE 802.11n

Grazie all'Access Point integrato, basato sulle più recenti specifiche 802.11n, è possibile realizzare reti wireless ad alte performance senza dover rinunciare ad un estesa copertura.

Completa eliminazione delle zone morte (grazie alle 2 antenne da 2 dBi) ed una velocità decisamente superiore alle attuali reti basate su standard 802.11b/g sono difatti le caratteristiche fondamentali di questa innovativa tecnologia di connessione wireless che garantisce prestazioni eccellenti in termini di throughput (sino a 300Mbps) senza dover rinunciare alla totale libertà di movimento.

La funzionalità WDS infine, utilizzando i più evoluti sistemi di sicurezza, permette, connettendo sino a 4 Access Point, di estendere la copertura wireless anche in zone remote.

Access point multipli virtuali

Il supporto Multi-SSID permette di creare sino a 4 Access Point virtuali con permessi di accesso diversificati alle risorse condivise. Il supporto client isolation (tra SSID diversi e tra client con lo stesso SSID) e VLAN tagging rende possibile emulare più access point virtuali.

Le dimensione compatte e il trasformatore integrato permettono un comodo montaggio a muro, rendendo il dispositivo di facile collocazione.

1.1 Requisiti di sistema

L'unico requisito indispensabile è un sistema operativo che integri lo stack TCP/IP ed una porta Ethernet con connettore RJ45 o interfaccia Wireless b/g/n. Nessun driver è richiesto per il funzionamento del dispositivo.

Prima di procedere con l'installazione del prodotto verificare inoltre quanto segue:

- Protocollo TCP/IP installato in ogni PC
- Un browser WEB quali Internet Explorer 5.0 o superiore, Netscape Navigator 6.0 o superiore

2. Contenuto della confezione

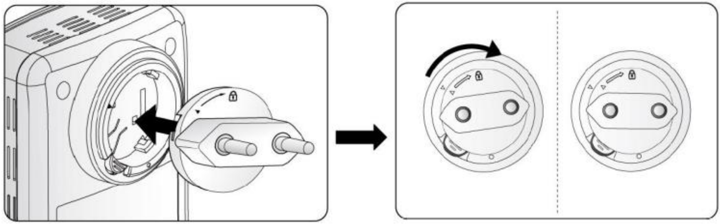
Una volta aperta la confezione in cartone dovrebbero essere presenti i seguenti componenti:

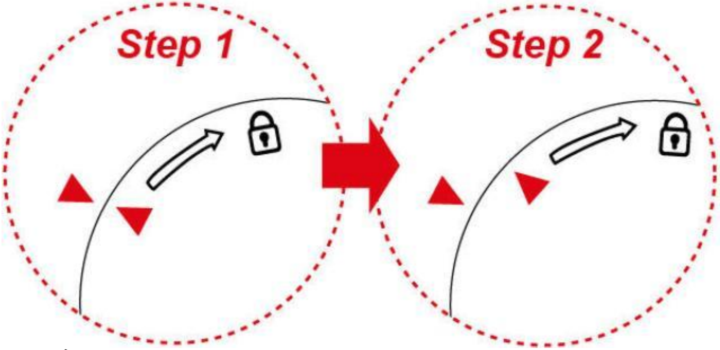
- NetFly AP3 WN
- Cavo di rete CAT-5 UTP (RJ45)
- Guida Rapida multilingua (Italiano, Francese ed Inglese)
- CD-Rom con Manualistica e documentazione
- Coupon di Garanzia e WEEE

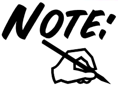
Qualora mancasse uno qualsiasi di questi componenti è necessario rivolgersi immediatamente al rivenditore.

3. Installazione hardware del dispositivo

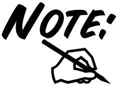
Anzitutto inserire nella parte posteriore del NetFly AP3 WN l'adattatore (per il collegamento alla presa elettrica) avendo cura che i 2 triangoli siano allineati (**STEP1**). A questo punto ruotare leggermente, nel verso indicato dalla freccia, per bloccare il meccanismo (**STEP2**).







E' opportuno non smontare frequentemente l'apparato al fine di evitare rotture meccaniche del dispositivo di inserzione della spina. Prestare la massima attenzione durante il processo.



Per rimuovere l'adattatore è opportuno anzitutto premere sul pulsante di sblocco e ruotare leggermente, nel verso contrario indicato dalla freccia e sino a che i 2 triangolini siano nuovamente allineati. A questo punto è possibile estrarre l'adattatore.

4. LED

NetFly AP3 WN dispone di 3 LED, 1 bottone WPS, tasto di reset ed una porta Ethernet.

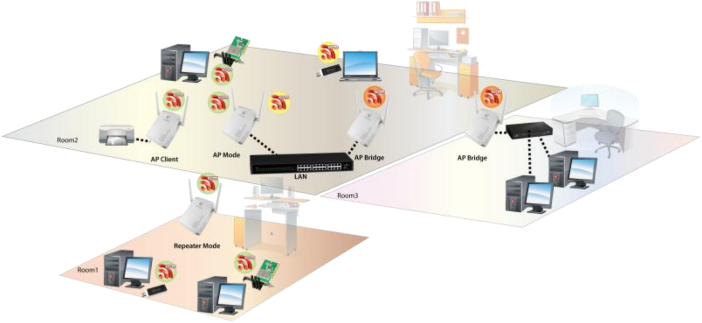


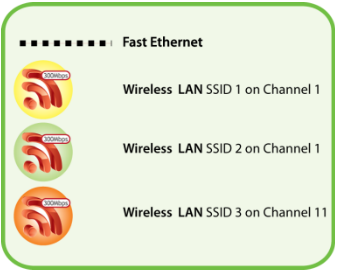
LED	INFORMAZIONE
WLAN	Acceso verde quando il Wireless è abilitato. Lampeggiante quando c'è trasferimento di dati. Lampeggiante (velocemente) quando la procedura WPS è attiva.
POWER	Acceso quando l'apparato è correttamente alimentato. Spento quando la tensione di rete è assente.
ETH	Acceso quando collegato ad un apparato ethernet. Lampeggiante durante trasferimento di pacchetti.

BOTTONE	UTILIZZO
WPS	Cliccare per lanciare la procedura di associazione automatica usando il WPS.
RESET	Premere il bottone di reset per almeno 3 secondi per effettuare il ripristino delle condizioni iniziali.

5. Cablaggio

Anzitutto collegare la porta RJ45 alla Lan e connettere il dispositivo direttamente nella presa elettrica. Una volta effettuati tutti i collegamenti il prodotto effettuerà una diagnostica la cui durata è di circa 2 minuti. Terminata questa fase il Led POWER sarà acceso verde fisso ed il i Led LAN/WLAN saranno accesi (a seconda dei collegamenti fatti) o lampeggianti.
In figura un esempio di installazione tipica in cui l'apparato viene utilizzato mostrando tutta la sua duttilità (come AP, in Multi SSID, come Client Wireless ed in modalità Bridge).





6. Settaggi di DEFAULT

Prima di iniziare la configurazione del dispositivo è necessario conoscere quali siano i settaggi di default. Lasciando questi settaggi e **impostando i PC come client DHCP** (come da istruzioni seguenti) è possibile utilizzare l'Atlantis NetFly AP3 WN in pochissimo tempo. Per una configurazione più dettagliata fare riferimento al manuale presente sul CD. Le configurazioni di default sono:

- Username:**admin**
- Password: **atlantis**
- Indirizzo IP LAN: (**192.168.1.252**), Subnet Mask (**255.255.255.0**)
- DHCP Server: abilitato (**192.168.1.10-192.168.1.50**)
- SSID= **A02-AP3-W300N**
- Channel=**6**, Autenticazione= **WPA2-PSK** con cifratura **AES** e password preimpostata: **NetFlyAP3WN**

7. Configurazione del BROWSER

Al fine di permettere la navigazione Internet tramite il NetFly, di seguito riportiamo la configurazione necessaria per i più comuni browser presenti sul mercato:

Internet Explorer 7/8

- Cliccare col tasto destro del mouse sull'icona e selezionare la voce **Proprietà**.

- Selezionare la scheda Connessioni e spuntare l'opzione **Non utilizzare mai connessioni remote**.

Mozilla Firefox 3.0

- Avviare il browser Mozilla Firefox
- Cliccare sulla **Strumenti** - >**Opzioni**
- Selezionare la sezione **Avanzate**
- Selezionare la scheda **Rete** -> **Connessioni**
- Cliccare su **Impostazioni** e selezionare l'opzione **Nessun Proxy**.

Google Chrome

- Avviare il browser Google Chrome.
- Cliccare sull'icona  e selezionare la voce **Opzioni**.
- Selezionare la scheda Roba da Smanettoni e successivamente l'opzione **Rete** -> **Modifica impostazioni Proxy**.

8. Configurazione del PC

Configurazione del PC in Windows 2000

- Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections.**
- Cliccare due volte su **Local Area Connection.**
- In **Local Area Connection Status/Wireless** cliccare **Properties.**
- Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties.**
- Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically.**
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows XP

- Andare su **Start** e poi **Panello di Controllo**. Cliccare due volte su **Connessione di rete** (se non fosse presente cliccare prima su: **Passa alla Visualizzazione Classica**).
- Cliccare due volte su **Connessione alla rete locale (LAN)/Wireless.**
- Nel TAB generale cliccare **Proprietà**.
- Selezionare **Protocollo Internet (TCP/IP)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente.**
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows Vista

- Andare su **Start** poi **Pannello di Controllo** (cliccare sulla voce **Visualizzazione classica**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione, poi** cliccare su **Gestisci connessione di rete.**
- Cliccare 2 volte sull'icona **Local Area Connection/Wireless** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).
- Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows 7

- Andare su **Start** poi **Pannello di Controllo** (cliccare sulla voce **Icone Piccole o Grandi**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione,** poi cliccare su **Modifica Impostazione Scheda.**
- Cliccare 2 volte sull'icona **Local Area Connection/Wireless** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).

- Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
- Premere su **OK** per terminare la configurazione.

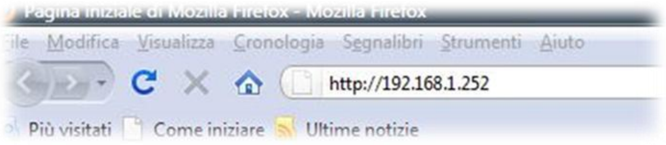
Configurazione del PC in MAC OS

- Cliccare sull'icona **Mela** nell'angolo in alto a sinistra dello schermo e selezionare: **Control Panel/TCP/IP**. Apparirà la finestra relativa al TCP/IP come mostrata in figura.
- Scegliere **Ethernet** in Connect Via.
- Scegliere **Using DHCP Server** in Configure.

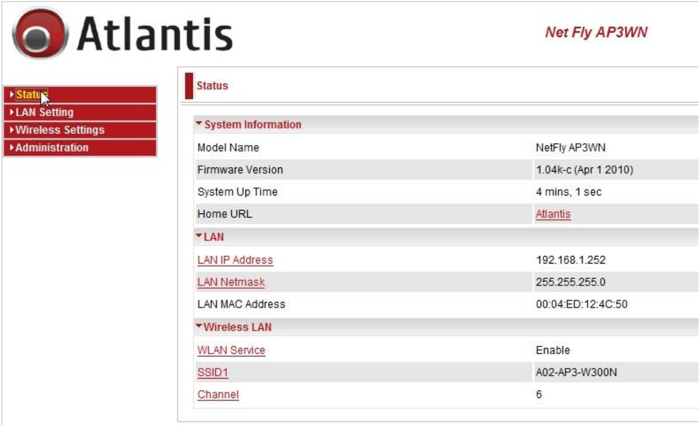
Lasciare vuoto il campo **DHCP Client ID**.

9. Configurazione via WEB

Digitare nel browser web il seguente indirizzo IP: **http://192.168.1.252** e premere il tasto invio.



Utilizzare **admin** (come nome utente) e **atlantis** (come password). Premere **OK** per continuare. Apparirà a questo punto il seguente menu:



L'interfaccia di configurazione è suddivisa nei seguenti sottomenù:

- **Status** [Status, Statistics]
- **LAN Settings** [LAN]
- **Wireless Settings** [Basic, Security, Advanced, WPS, VLAN, Station List]

- **Administration** [Management, Firmware Upgrade, Settings Management, Restart]

A questo punto è possibile cambiare **l'indirizzo IP** dell'apparato nella sezione **LAN**, la **password di accesso** in **Administration->Management** e la configurazione della sezione Wireless (modalità e sicurezza) nei sottomenu **Wireless Settings.**
Per una configurazione dettagliata fare riferimento al manuale presente su CD.

NOTE!

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11g/b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6).
Da questo si evince che soltanto 3 Access Point/Wireles Router in standard g (o in N con canale da 20Mhz) possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali (funzionamento contemporaneo).

NOTE!

La selezione errata della regione (nel campo Country Region) potrebbe portare ad un utilizzo di frequenze vietate. E' necessario scegliere la regione corretta.

NOTE!

Il WEP viene oggi considerata non come assolutamente sicura e pertanto laddove possibile si consiglia l'uso del WPA.

9.1 Status -> Status

In questa sezione, sarà possibile visualizzare tutti i dettagli relativi alle configurazioni dell’apparato.



SYSTEM INFORMATION

PARAMETRO	SIGNIFICATO
Model Name	Indica il modello del dispositivo
Firmware Version	Indica la versione di firmware attualmente utilizzata dal dispositivo. E’ buona norma, al momento della prima installazione, verificare la disponibilità di firmware aggiornati sul sito web www.atlantis-land.com alla relativa sezione di prodotto.
System Up Time	Indica il tempo di attività del dispositivo dal momento dell’ultima accensione.

LAN

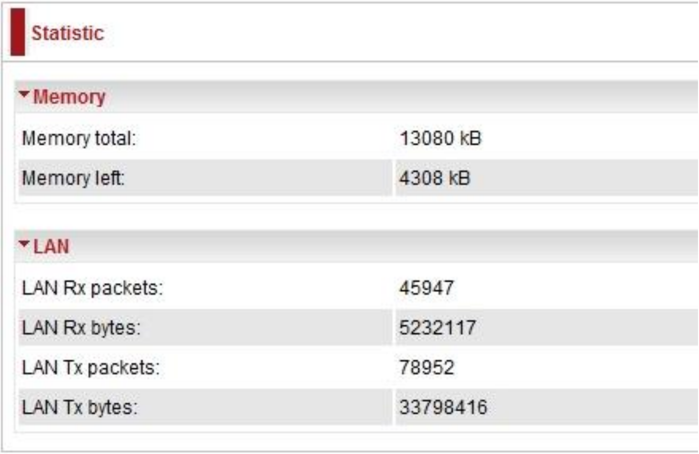
PARAMETRO	SIGNIFICATO
LAN IP Address	Indica l’indirizzo IP primario associato al dispositivo.

LAN Netmask	Indica la maschera di rete associata all'indirizzo IP primario riportato nel campo **LAN IP Address**.
LAN MAC Address	Indica l'indirizzamento fisico (MAC Address) associato all'interfaccia LAN del dispositivo.

WIRELESS LAN

PARAMETRO	SIGNIFICATO
WLAN Service	Indica lo stato di attività del modulo radio integrato.
SSID	Visualizza il nome identificativo della rete wireless fornita dall'apparato.
Channel	Indica il canale correntemente utilizzato dall'AP per la comunicazione radio.

9.2 Status -> Statistics



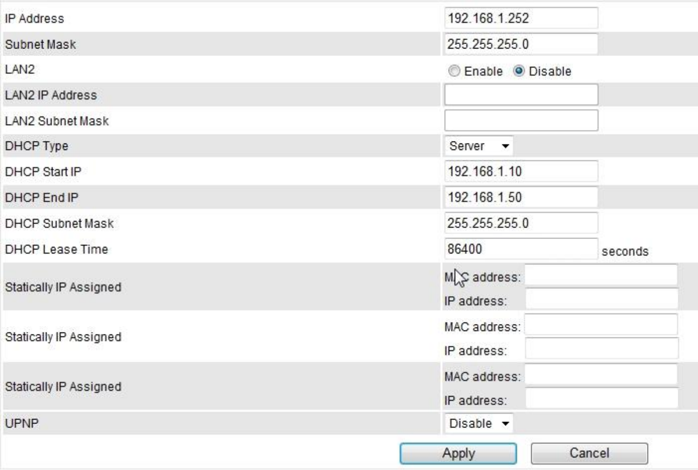
MEMORY

PARAMETRO	SIGNIFICATO
Memory Total	Indica il valore totale della memoria disponibile (in Bytes).
Memory Left	Indica il valore della memoria attualmente utilizzata dal dispositivo (in Bytes).

LAN

PARAMETRO	SIGNIFICATO
LAN Rx Packets	Indica il numero di pacchetti ricevuti sull'interfaccia LAN da parte del dispositivo.
LAN Rx Bytes	Indica il numero di bytes ricevuti sull'interfaccia LAN da parte del dispositivo.
LAN Tx Packets	Indica il numero di pacchetti trasmessi dall'interfaccia LAN del dispositivo.
LAN Tx Bytes	Indica il numero di bytes trasmessi dall'interfaccia LAN del dispositivo.

9.3 LAN Settings -> LAN



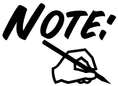
LAN SETUP

PARAMETRO	SIGNIFICATO
IP Address	Inserire l'indirizzo IP primario che si desidera assegnare all'apparato.
Subnet Mask	Inserire la maschera di rete relativa all'indirizzo IP inserito nel campo **IP Address**.
LAN2	Selezionare **Enable** per attivare la creare di una seconda interfaccia IP virtuale. In questo modo, è possibile di assegnare un secondo indirizzo IP al dispositivo per consentire la comunicazione tra 2 reti e/o nodi differenti. Mantenere la selezione su **Disable** nel caso in cui la funzionalità non sia necessaria.
LAN2 IP Address	Inserire l'indirizzo IP da assegnare all'interfaccia LAN virtuale.
LAN2 Subnet Mask	Inserire la maschera di rete relativa all'indirizzo IP immesso nel campo **LAN2 IP Address**.
DHCP Type	Permette di abilitare o disattivare la funzionalità DHCP Server. Selezionare l'opzione **Server** per attivare la funzione e

	configurare i parametri relativi oppure **Disable** nel caso in cui tale funzionalità non sia necessaria.
UPnP	Abilita (**Enable**) o disabilita (**Disable**) il supporto Universal Plug'n'Play da parte del dispositivo.

DHCP SERVER (disponibili solo se attivato)

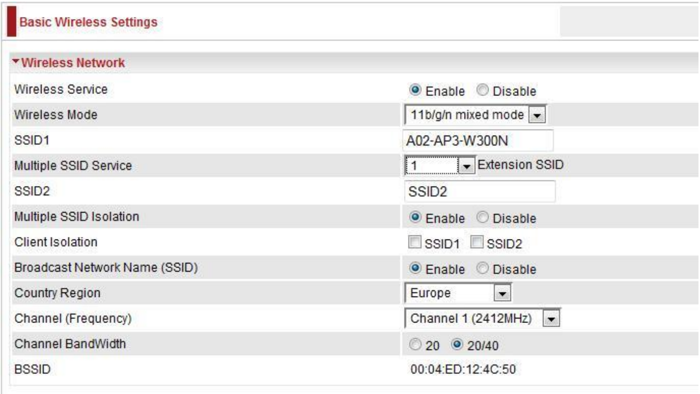
PARAMETRO	SIGNIFICATO
DHCP Start IP	Inserire l'indirizzo iniziale del pool di indirizzi che il server DHCP adrà a rilasciare in caso di richiesta di lease da parte dei terminali.
DHCP End IP	Inserire l'indirizzo finale del pool di indirizzi che il server DHCP andrà a rilasciare in caso di richiesta di lease da parte dei terminali.
DHCP Subnet Mask	Inserire la maschera di rete, relativa al pool di indirizzi specificato nei campi **DHCP Start IP** e **DHCP End IP**, che il server DHCP andrà a rilasciare in caso di richiesta di lease da parte dei terminali.
DHCP Lease Time	Indicare il perido di validità dell'indirizzo rilasciato dal server DHCP. Al termine di questo intervallo, è necessario eseguire nuovamente la richiesta di rilascio da parte del terminale.
Statically IP Assigned (1-3)	Indicare nei campi **MAC Address** ed **IP Address** gli indirizzi necessario per la creazione di una policy di assegnazione statica. In questo modo, al momento della richiesta di rilascio di un indirizzo IP da parte di uno specifico indirizzo MAC, ad esso verrà assegnato l'indirizzo IP contenuto nel campo **IP Address**.
UPnP	Si veda l'opportuna appendice.



Gli indirizzi inseriti nella sezione **Statically IP Address** non devono essere compresi all'interno del range di indirizzi assegnato dal DHCP.
Tale range è definito, nel suo limite inferiore dal valore del campo **DHCP Start IP** e nel suo margine superiore dal valore indicato nel campo **DHCP End IP**.
Sono configurabili sino a **3 IP statici** (assegnati in DHCP in

maniera statica quando la richiesta viene fatta da un determinato Mac Address).

9.4 Wireless Setting -> Basic



WIRELESS NETWORK

PARAMETRO	SIGNIFICATO
Wireless Service	Permette di abilitare/disabilitare il modulo radio integrato nel dispositivo. Selezionare **Enable** per abilitare il modulo Wireless, selezionare **Disable** per stoppare tale modulo.
Wireless Mode	Permette di selezionare la modalità operativa in maniera tale da rendere la rete wireless compatibile anche con dispositivi basati su standard precedenti (IEEE802.11b/g) oppure renderla funzionante su di un esclusiva modalità operativa, escludendo di fatto tutti i dispositivi basati su standard differenti. Nello specifico, è possibile utilizzare il dispositivo secondo le modalità indicate: • **11b/g/n mixed mode:** questa modalità d'uso, attiva per default, garantisce il più alto grado di compatibilità dell'apparato con la maggior parte dei dispositivi in commercio, anche se basati su standard precedenti. • **11b/g mixed mode:** permette all'apparato di

	dialogare con dispositivi basati sui precedenti standard IEEE 802.11b/g, escludendo di fatto la comunicazione con i client più recenti basati sul protocollo IEEE 802.11n. • **11g only:** permette all'apparato di dialogare esclusivamente con dispositivi basati sullo standard IEEE 802.11g, escludendo di fatto tutto ciò che è basato su standard precedenti (IEEE 802.11b) e successivi (IEE 802.11g). • **11b only:** permette all'apparato di dialogare esclusivamente con dispositivi basati sullo standard IEEE 802.11b, escludendo di fatto tutto ciò che è basato su standard successivi (IEE 802.11g/n).
Network Name (SSID1) (SSID2) (SSID3) (SSID4)	Inserire il nome identificativo della rete wireless (Service Set Identifier) ed in tutti i client wireless che dovranno essere connessi. Il parametro è Case-Sensitive e non deve superare i 32 caratteri. Il nome contenuto in questo campo verrà visualizzato dai client wireless durante la scansione delle reti disponibili.
Multiple SSID Service	In questa sezione è possibile generare altri 3 profili SSID da affiancare al profilo principale. Selezionare, dalla combo-box il numero di SSID aggiuntivi da utilizzare. Selezionare **Disable** per utilizzare solo l'SSID principale. Il dispositivo può supportare sino a 4 diversi SSID (in questo caso selezionare **3**) ciascuno con profili di autenticazione diversi.
Multiple SSID Isolation	Spuntare **Enable** per isolare i client appartenenti ad SSID diversi (i client loggati a diversi SSID non potranno comunicare tra loro). Spuntare **Disable** per permettere la comunicazione tra client connessi a SSID diversi.
Client Isolation	Spuntare **Enable** per isolare i client loggati allo stesso SSID tra loro. Spuntare **Disable** per permettere la comunicazione tra client connessi allo stesso SSID.
Broadcast Network Name (SSID)	Permette di abilitare/disabilitare la visualizzazione dell'SSID di rete durante le operazioni di scansione delle reti wireless da parte dei client. Selezionare **Enable** se si desidera che il nome della rete venga visualizzato, oppure **Disable** per nasconderlo. Nel caso in cui l'opzione sia impostata su **Disable**, ogni client

	che desideri collegarsi alla rete fornita da NetFly AP3 WN deve conoscere preventivamente l'SSID della stessa.
Country Region	Viene mostrata la regione di funzionamento selezionata. Ad ogni regione sono associate determinate frequenze utilizzabili. Selezionare **Europe.**
Frequency (Channel)	Permette la selezione del canale di comunicazione utilizzato dall'Access Point. Selezionare manualmente un canale libero (da 1 a 13 secondo lo standard ETSI) da interferenze oppure selezionare **AutoSelect** per permettere al dispositivo di scegliere in maniera autonoma il miglior canale disponibile. Per maggiori informazioni sulla selezione del miglior canale disponibile, fare riferimento all'appendice specifica.
Channel Bandwidth	Permette la selezione dell'ampiezza di canale da utilizzare. Mentre per gli standard precedenti (IEEE 802.11b/g) l'ampiezza massima utilizzabile per singolo canale è di 20MHz, il nuovo standard IEEE802.11n permette di utilizzare fino al doppio dell'ampiezza per singolo canale (40MHz), introducendo altresì una modalità di riduzione dello stesso a 20 MHz in caso di rilevazione di interferenze. Selezionare **20** per forzare l'ampiezza massima di canale a 20MHz (configurazione adatta per ambienti molto rumorosi) oppure **20/40** per permettere al dispositivo di utilizzare un canale da 40MHz (se possibile). Resta inteso che, nel caso in cui si selezioni l'opzione **20/40**, client basati su standard precedenti comunicheranno con il dispositivo utilizzando l'ampienzza massima consentita dallo standard in uso.
BSSID	Indica l'indirizzo MAC associato alla rete wireless identificata dall'SSID riportato nel campo **Network Name (SSID)**
WDS	Permette di abilitare la funzionalità WDS (Wireless Distribution System) in una delle modalità supportate dal prodotto (**Lazy Mode**, **Bridge Mode** o **Repeat Mode**).

NOTE:

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11n/g/b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6).
Da questo si evince che soltanto 3 Access Point/Wireless Router possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali (funzionamento contemporaneo).
La modalità 802.11n inoltre prevede un canale più ampio a 40Mhz (in questo caso solo 2 AP possono operare nelle condizioni di sopra, utilizzando rispettivamente il canale basso e alto).

NOTE:

La selezione errata della regione (nel campo **Country Region**) potrebbe portare ad un utilizzo di frequenze vietate. E' necessario scegliere la regione corretta.

NOTE:

Si sconsiglia l'uso del WEP e si raccomanda vivamente l'uso del WPA.

WDS

La tecnologia WDS (Wireless Distribution System) permette di mettere in comunicazione 2 o più punti di accesso, in modo da creare un infrastruttura di trasporto wireless, senza la richiesta di alcun cablaggio.

E' importante ricordare che la tecnologia WDS non è sottoposta ad alcuna attività di standardizzazione e pertanto è garantita solo tra apparati identici.

NetFly AP3 WN supporta 3 differenti modalità di configurazione per quanto riguarda la parte WDS:

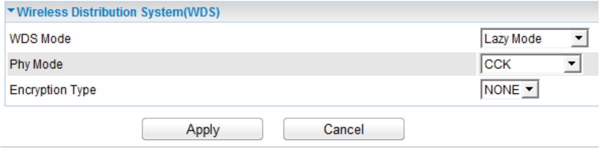
- **Lazy Mode:** In questa modalità, eventuali apparati WDS remoti vengono automaticamente rilevati.
- **Bridge Mode:** In tale modalità, il NetFly AP3 WN funzionerà in modalità bridge, stabilendo un collegamento wireless con altri AP di cui verranno indicati gli indirizzi MAC.

Si ricorda che, nel caso di configurazione in modalità Bridge, l'apparato non funzionerà in modalità Access Point, rifiutando di fatto qualsiasi richiesta da MAC Address differenti da quelli indicati come WDS Peer.

- **Repeat Mode:** In questa modalità, il NetFly AP3 WN funzionerà in modalità repeater come l'estensione di una rete wireless già esistente.

Si ricorda che, nel caso di configurazione in modalità Repeater, è previsto un significativo degrado delle prestazioni velocistiche della rete wireless.

NetFly AP3 WN è in grado di supportare un massimo di 4 link WDS contemporanei.
Si ricorda inoltre che, per ciascuna delle modalità sopra indicate, è necessario che la comunicazione WDS avvenga tra apparati identici. E' assolutamente sconsigliato utilizzare NetFly AP3 WN in modalità WDS con apparati differenti e/o di altre marche.



WDS->Lazy Mode

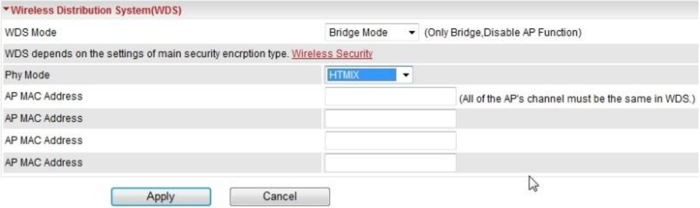
In questa modalità, eventuali apparati WDS remoti vengono automaticamente rilevati. L'AP funziona contemporaneamente in Bridge ed Access Point.



PARAMETRO	SIGNIFICATO
WDS Mode	Selezionare l'opzione **Lazy Mode** per permettere all'apparato di avviare il processo di autoriconoscimento dei peer WDS remoti.

WDS->Bridge Mode

tale modalità, il NetFly AP3 WN funzionerà in modalità bridge, stabilendo un collegamento wireless con altri AP di cui verranno indicati gli indirizzi MAC. Si ricorda che, nel caso di configurazione in modalità Bridge, l'apparato non funzionerà in modalità Access Point, rifiutando di fatto qualsiasi richiesta da MAC Address differenti da quelli indicati come WDS Peer.



PARAMETRO	SIGNIFICATO
WDS Mode	Selezionare l'opzione **Bridge Mode** per permettere all'apparato di avviare il processo di autoriconoscimento dei peer WDS remoti.
Phy Mode	Selezionare la modalità desiderata dal menu a tendina tra: • **CCK** • **OFDM** • **HTMIX** • **GREENFIELD** E' fondamentale che la medesima modalità sia impostata sul peer WDS remoto con il quale si intende comunicare.
AP MAC Address	Inserire fino a 4 indirizzi MAC con i quali si desidera stabilire un collegamento WDS. Per consentire la comunicazione, è necessario che ciascuno dei peer remoti indicati contenga a sua volta l'indirizzo MAC dell'apparato locale.
Encryption Type (in Wireless Security)	Selezionare l'algoritmo di crittografia da utilizzare per la cifratura del traffico veicolato sul link WDS. E' possibile selezionare un opzione tra le seguenti: • **WEP** • **TKIP** • **AES** E' fondamentale che la medesima modalità sia impostata sul peer WDS remoto con il quale si intende comunicare.

Encryption Key (in Wireless Security)	Inserire la chiave precondivisa da utilizzare per l'autenticazione e la crittografia dei dati.

WDS->Repeater Mode

In questa modalità, il NetFly AP3 WN funzionerà in modalità repeater come l'estensione di una rete wireless già esistente.



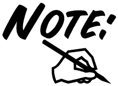
PARAMETRO	SIGNIFICATO
WDS Mode	Selezionare l'opzione **Repeat Mode** per permettere all'apparato di avviare il processo di autoriconoscimento dei peer WDS remoti.
AP MAC Address	Inserire fino a 4 indirizzi MAC con i quali si desidera stabilire un collegamento WDS. Per consentire la comunicazione, è necessario che ciascuno dei peer remoti indicati contenga a sua volta l'indirizzo MAC dell'apparato locale.
Encryption Type (in Wireless Security)	Selezionare l'algoritmo di crittografia da utilizzare per la cifratura del traffico veicolato sul link WDS. E' possibile selezionare un opzione tra le seguenti: • **WEP** • **TKIP** • **AES** E' fondamentale che la medesima modalità sia impostata sul peer WDS remoto con il quale si intende comunicare.
Encryption Key (in Wireless Security)	Inserire la chiave precondivisa da utilizzare per l'autenticazione e la crittografia dei dati. E' fondamentale che la medesima modalità sia impostata sul peer WDS remoto con il quale si intende comunicare.

9.5 Wireless Setting -> Security

In questa sezione, è possibile configurare la policy di sicurezza che si desidera applicare alla rete wireless (ciascun SSID può avere differente policy di sicurezza wireless), nonché dichiarare il permesso/inibizione di collegamento di determinati indirizzi MAC alla rete wireless del NetFly AP3 WN.



PARAMETRO	SIGNIFICATO
SSID Choice	Selezionare l'SSSID di cui si vuole definire la sicurezza.
Security Mode	Selezionare l'algoritmo crittografico da utilizzare.



Si ricorda che il prodotto, per impostazione di fabbrica, è configurato con un algoritmo di crittografia WPA-PSK, la cui chiave precondivisa è riportata nella sezione "Impostazioni di fabbrica" del presente manuale.

NetFly AP3 WN supporta i più recenti standard di sicurezza (WPA/WPA2-PSK in AES) nonché un algoritmo di crittografia a chiave statica (WEP) per garantire la compatibilità del prodotto con client datati e/o obsoleti.

WEP (Wired Equivalent Privacy)

L’algoritmo di sicurezza WEP è un algoritmo di crittografia ed autenticazione a chiave statica.
Basato su protocollo RC-4, è possibile individuare la sua principale debolezza nell’utilizzo di una medesima chiave statica precondivisa sia per la parte di autenticazione dei client che per le operazioni di cifratura del traffico.
Sostituito dal più recente WPA (WiFi Protected Access), rimane comunque il pioniere dei protocolli di sicurezza per quanto riguarda le wireless LAN ed è il solo protocollo supportato dai client basati su standard IEEE802.11b.



PARAMETRO	SIGNIFICATO
Security Mode	Selezionare un opzione tra quelle di seguito riportate: • **WEP Shared:** Utilizzare questa modalità nel caso in cui si desideri creare un sistema basato su WEP a chiave condivisa. • **WEP Open:** Utilizzare questa modalità nel caso in cui si desideri creare un sistema basato su WEP a chiave aperta. • **WEP AUTO:** Utilizzare questa modalità nel caso in cui si desideri che l’apparato selezioni in maniera automatica la modalità operativa da utilizzare (Shared od Open).
Default Key	Selezionare quale tra le 4 chiavi inserite nel campi **WEP Keys** si desidera utilizzare per la crittografia dei dati.
WEP Keys	Inserire fino a 4 chiavi da utilizzare per la fase di autenticazione/crittografia dei dati. E’ possibile inserire ogni singola chiave in formato esadecimale (HEX – da 0 a 9 e da A ad F), oppure in formato ASCII.

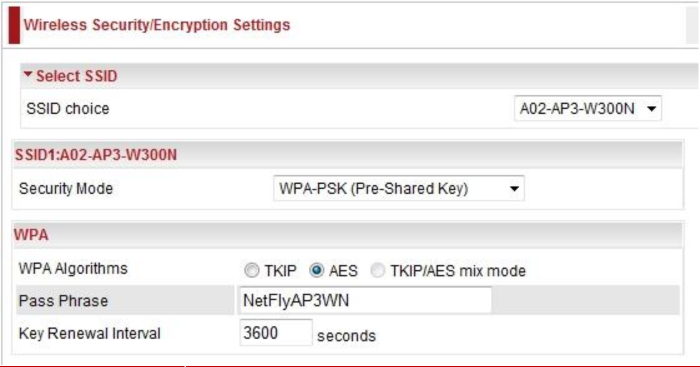
NOTE:

Si ricorda che esistono alcune limitazione in merito alla lunghezza delle chiavi utilizzabili dall'algoritmo WEP. Riportiamo di seguito le limitazioni per ogni tipologia di immissione:

- **WEP 64-bits:** 5 caratteri ASCI o 10 coppie esadecimali
- **WEP 128-bits:** 13 caratteri ASCII o 26 coppie esadecimali

WPA-PSK/WPA2-PSK (Wifi Protected Access)

L’algoritmo di sicurezza WPA è un algoritmo di crittografia ed autenticazione a chiave dinamica.
Anch’esso basato su protocollo RC-4, utilizza una chiave precondivisa per la fase di autenticazione dei client alla rete e per la fase iniziale di crittografia dei dati. Successivamente, al termine di un intervallo impostabile dall’utente, la BSE provvede a comunicare a tutti i client autenticati e collegati la nuova chiave da utilizzare per la crittografia dei dati.
Questo protocollo, supportato ormai da tutti i client disponibili sul mercato basati su standard IEEE802.11g o superiore, ha subito un ulteriore incremento del livello di sicurezza nella sua release WPA2, grazie all’introduzione della crittografia secondo protocollo AES (attualmente il protocollo più sicuro presente sul mercato).
NetFly AP3 WN supporta i 2 protocolli sopra descritti sia singolarmente che in una modalità ibrida, dove sarà il dispositivo stesso ad utilizzare il più alto standard di sicurezza supportato dai vari client collegati in rete.

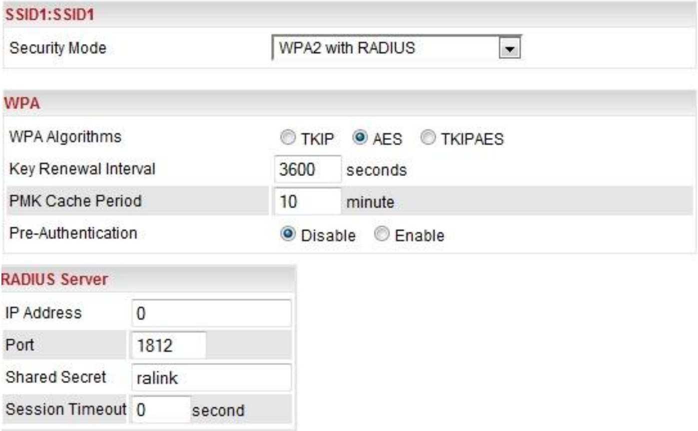


PARAMETRO	SIGNIFICATO
Security Mode	Selezionare un opzione tra quelle di seguito riportate: • **WPA-PSK:** Selezionare questa modalità per utilizzare esclsuviamente l’algoritmo WPA-PSK. • **WPA2-PSK:** Selezionare questa modalità per utilizzare esclsuviamente l’algoritmo WPA2-PSK. • **WPAPSK/WPA2PSK mix mode:** Selezionare questa modalità per utilizzare il più alto standard di sicurezza supportato dai vari client presenti in rete.

	• **WPA/WPA2 con RADIUS:** Permette di utilizzare un server Radius (si veda il paragrafo seguente).
WPA Algorithms	Selezionare l'algoritmo da utilizzare tra le modalità esclusive **TKIP** ed **AES**, oppure la modalità ibrida **TKIP/AES**.
Pass Phrase	Inserire la chiave precondivisa necessaria per l'autenticazione dei client.
Key Renewal Interval	Inserire il valore dell'intervallo (espresso in secondi) al termine del quale verrà eseguito il rinnovo della chiave crittografica. Generalmente, più basso è l'intervallo e più risulta alto il grado di sicurezza della rete, a scapito però delle prestazioni velocistiche di quest'ultima.

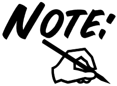
WPA/WPA2 with RADIUS

Un server Radius viene utilizzato per autenticare un client e reinviargli i parametri per l'accesso al network wireless. RADIUS (Remote Authentication Dial-In User Service) utilizza un server RADIUS per l'autenticazione e poi un algoritmo per la cifratura (WEP, TKIP o AES) dei dati.



PARAMETRO	SIGNIFICATO
Security Mode	Selezionare un opzione tra quelle di seguito riportate: • **WPA2 with RADIUS:** Selezionare questa modalità per utilizzare esclusivamente l'algoritmo WPA2. • **WPA with RADIUS:** Selezionare questa modalità per utilizzare esclusivamente l'algoritmo WPA.
WPA Algorithms	Selezionare l'algoritmo da utilizzare tra le modalità esclusive **TKIP** ed **AES**, oppure la modalità ibrida **TKIP/AES**.
Key Renewal Interval	Inserire il valore dell'intervallo (espresso in secondi) al termine del quale verrà eseguito il rinnovo della chiave crittografica.
PMK Cahce Period/ Pre-Authentication	Utilizzo facoltativo della memorizzazione nella cache PMK (Pairwise Master Key) e la memorizzazione nella cache PMK opportunistico. Nella memorizzazione nella cache PMK, i client

	senza fili e senza fili accesso punti cache i risultati delle 802.1X autenticazioni. Di conseguenza, l'accesso è molto più veloce quando un client wireless ritorna a un accesso senza fili scegliere che il client già autenticato.
IP Address	Introdurre l'indirizzo IP della macchina Radius.
Port	Introdurre il numero di porta utilizzata dalla macchina Radius, solitamente la 1812.
Shared Secret	Inserire la chiave precondivisa necessaria per l'autenticazione dei client.
Session Timeout	Introdurre in secondi la durata della sessione (dopo inattività verrà interrotta). Lasciare 0 per evitare questo time-out.

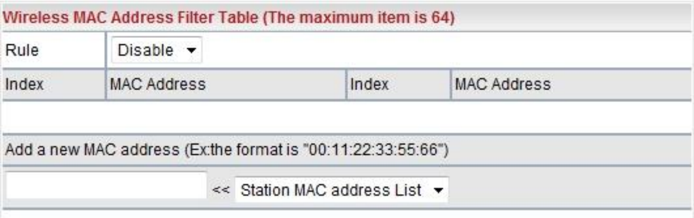


Si sconsiglia l'autenticazione Radius quando si utilizzano SSID multipli.

Access Policy

In questa sezione, è possibile definire una policy di filtraggio a livello MAC, cosi da inibire l'accesso alla rete da parte di determinati client dichiarati. NetFly AP3 WN è in grado di offrire 2 differenti policy di filtraggio:

- **Allow Policy:** Permette l'accesso alla rete dei soli clienti indicati, bloccando tutto ciò che non è espressamente dichiarato come permesso.
- **Reject Policy:** Permette l'accesso alla rete a tutti i client, ad esclusione di quelli espressamente indicati.



PARAMETRO	SIGNIFICATO
Rule	Selezionare la policy desiderata tra **Disable, Allow** e **Reject**. Per maggiori informazioni, si prega di fare riferimento a quanto indicato appena sopra.
Add a station MAC address	Inserire l'indirizzo MAC del client che si desidera consentire/bloccare, sulla base della policy selezionata nel campo **Policy**.

9.6 Wireless Setting -> Advanced

In questa sezione, è possibile configurare alcuni parametri avanzati, utilizzati per le operazioni di “fine-tuning” della rete wireless.



ADVANCED SETTINGS

PARAMETRO	SIGNIFICATO
TX Power	Selezionare la percentuale di potenza da utilizzare per l’attività di trasmissione della parte radio. In caso di ambienti molto rumorosi, potrebbe essere indicato diminuire la potenza trasmissiva, al fine di migliore la qualità della comunicazione.
TX Burst	Permette di abilitare il burst dei pacchetti per ottenere un throughput più elevato (deve essere supportato anche dai client collegati).

WI-FI MUltimedia

PARAMETRO	SIGNIFICATO
WMM	Abilitando questa caratteristica è possible per controllare la priorità di accesso di 4 categorie di servizi: Voice, Video, Best Effort and Background. Il valore di default è **Enable.**
APSP	Automatic Power Save Delivery (APSD) è un sistema di controllo degli stati di attività. Se attivo permette all'apparato di escludere talune funzionalità offrendo un risparmio sui consumi. Il valore di default è **Enable.**

IGMP Snooping

PARAMETRO	SIGNIFICATO
IGMP Snooping Service	Permette di abilitare o meno il servizio IGMP. Il valore di default è **Enable**

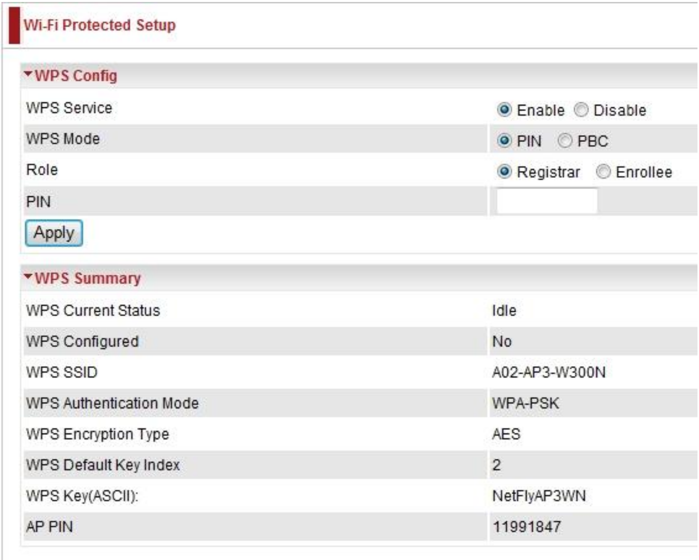
Tradizionalmente i pacchetti IP vengono trasmessi in Unicast (1 trasmittente – 1 ricevente) oppure in Broadcast (1 trasmittente – tutta la rete). Il Multicast permette di inviare pacchetti ad un gruppo definito di hosts sulla rete.
L'IGMP (Internet Group Multicast Protocol) è un protocollo utilizzato per stabilire una relazione di appartenenza in un gruppo Muticast – non è utilizzato per trasportare dati dell'utenza. L'IGMP versione 2 (RFC 2236) è un'implementazione perticolare della versione 1 (RFC 1112) che resta ancora largamente utilizzata. Per maggiori dettagli sull'interoperabilità tra i protocolli IGMP versione 1 e 2 è possibile consultare le sezioni 4 e 5 dell' RFC 2236. Gli indirizzi IP di classe D sono utilizzati per identificare un gruppo di hosts e si trovano nel range da 224.0.0.0 a 239.255.255.255.
L'indirizzo IP 224.0.0.0 non è assegnato ad alcun gruppo, è utilizzato da computers con IP Multicast. L'indirizzo 224.0.0.1 è utilizzato per messaggi di richiesta ed è assegnato al gruppo permanente di tutti gli indirizzi IP (inclusi i gateways). Tuti gli hosts devono appartenere al gruppo 224.0.0.1 per partecipare alla comunicazione IGMP. Il WebShare Wireless ADSL2+ Router supporta entrambe le versioni del protocollo IGMP. Allo Start-Up il Router interroga tutte le reti a lui direttamente connesse per identificare le appartenenze ai gruppi.
Fatto ciò, il dispositivo aggiorna periodicamente queste informazioni.

9.7 Wireless Setting -> WPS

Il prodotto supporta pienamente le specifiche Wi-Fi Protected Setup, al fine di consentire una semplice installazione della rete wireless.
Questo insieme di specifiche prevede che le fasi di sincronizzazione e messa in sicurezza della WLAN vengano gestite in maniera autonoma dai dispositivi che supportino tali funzionalità.
Nello specifico, WPS prevede 2 modalità di sincronizzazione tra il punto di accesso ed i relativi client: la prima prevede la pressione di un apposito pulsante sul punto di accesso e successivamente su tutti i client appartenenti alla stessa wireless network. Questa procedura avvierà un processo di sincronizzazione automatica durante il quale i prodotti, oltre che all' autenticazione presso il punto di accesso, negozieranno una chiave di sicurezza (secondo gli standard supportati dai vari client) per la messa in sicurezza della rete. Al termine della procedura la rete wireless sarà così configurata e pronta per essere utilizzata.
La seconda prevede che la fase di autenticazione dei client sul punto di accesso avvenga tramite il riconoscimento di un codice PIN univoco associato al client, mentre tutta la parte successiva di messa in sicurezza sarà identica alla modalità illustrata sopra. Esistono 2 modalità di autenticazione (Enrollee o Registar) in base al dispositivo che si occuperà di gestire la fase iniziale di autenticazione.
Nello specifico, vediamo ora come configurare le 2 modalità di associazione WPS sul NetFly AP3 WN.

WPS PIN Setup (Enrollee o Registar Mode)

1. Identificare il codice WPS PIN sul client wireless che si desidera associare al prodotto.
2. Accedere alla sezione WPS del NetFly AP3 WN ed impostare i parametri come da figura:



3. Inserire il PIN rilevato secondo le modalità indicate al punto uno nel campo **Enrollee's PIN**.

4. Accedere alla configurazione del client wireless ed impostare il PIN indicato nel campo **AP PIN** come codice per l'autenticazione del punto di accesso.

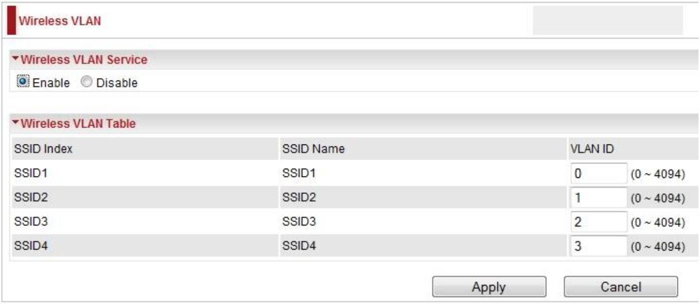
WPS Button Setup

1. Premere il pulsante WPS posto sulla parte superiore del NetFly AP3 WN; il led Wireless comincerà a lampeggiare in maniera regolare.

2. Premere il pulsante WPS sul client o sui client che si desidera far autenticare al NetFly AP3 WN entro 120 secondi.

In alcune tipologie di client, il pulsante WPS può non essere presente; si prega di consultare il manuale utente per la verifica del supporto di questa tecnologia e per l'eventuale modalità di attivazione.

9.8 Wireless Setting -> VLAN



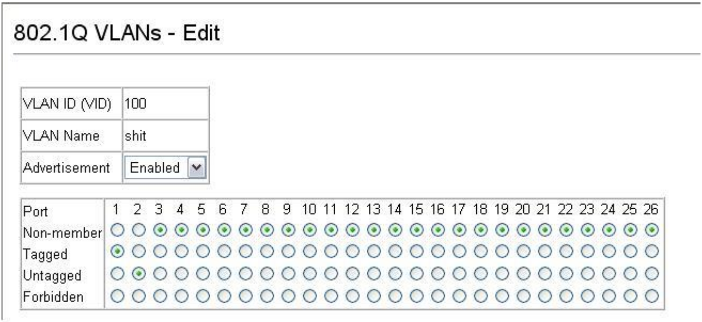
Spuntare **Enable,** per attivare la funzionalità VLAN.
E' possibile associare ad ogni SSID un valore (nel campo VLAN ID) diverso scelto tra 0-4094. E' opportuno verificare che l'intera infrastruttura di rete sia in grado di gestire il tagging VLAN dei pacchetti.

E' opportuno considerare che dopo l'abilitazione del VLAN tagging, il dispositivo può essere configurato solo alle seguenti condizioni:

- Via wireless tramite l'SSID1.
- Tramite uno switch con capacità di tag/untag VLAD ID.
- Tramite uns scheda di rete con capacità di tagging/untagging dei pacchetti.

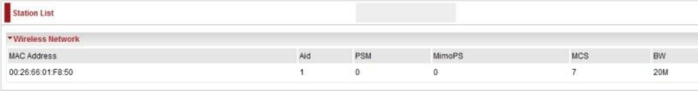
VLAN ESEMPIO

Si voglia effettuare il seguente esempio di configurazione.
Si voglia permettere ai soli client connessi all'SSID 1 di accedere al servizio X.
SSID1->VLAN ID=100
Il NetFly AP3 WN, per ogni pacchetto proveniente, dall'SSID 1 applicherà la marcatura VLAN ID=100 e lo invierà alla porta Ethernet.
Questa porta Ethernet è collegata alla porta 1 di uno Switch capace di gestire il TAG/UNTAG su VLAN.
La porta 2 dello switch è collegata al servizio



Atlantis

9.9 Wireless Setting -> Station List


Station List

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW
00:26:66:01:F8:50	1	0	0	7	20M

Wireless

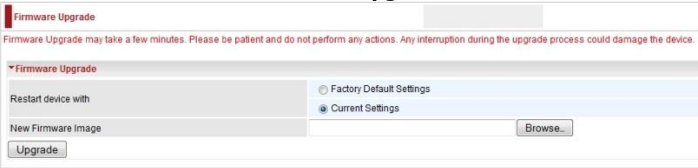
Parametro	Descrizione
MAC Address	Indica l'indirizzo MAC associato ad ogni indirizzo IP contenuto nel campo **IP Address**.
AID	Indica l'ID di associazione.
PSM	La modalità Power Save Mode.
MimoPS	Modalità MIMO Power Save. Se utilizzata da entrambi gli apparati (trasmittente e ricevente) migliora drasticamente le prestazioni ottenibili.
MCS	Indica modulazione e tipo di codice utilizzato. Si faccia riferimento per ulteriori dettagli ad IEEE802.11n.
BW	L'ampiezza di canale. Può essere 20Mhz o 40Mhz.

9.10 Administration -> Management

Al fine di prevenire accessi non autorizzati all'interfaccia di configurazione del prodotto, è necessario cambiare il prima possibile la password di accesso.
Tramite questa sezione è possibile modificare la password dell'account esistente.
Inserire nel campo password la nuova password e cliccare poi su **Apply.**



9.11 Administration -> Firmware Upgrade

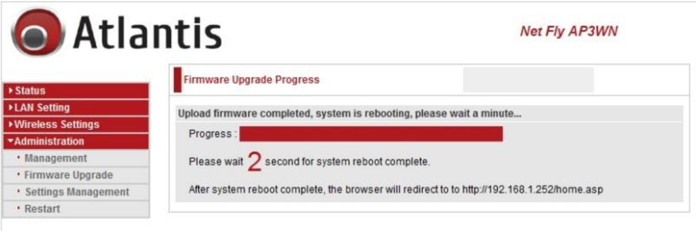


Per effettuare l'upgrade del firmware del dispositivo è necessario anzitutto scaricare dal sito **www.atlantis-land.com** (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù **Administration-> Firmware Upgrade** e premere poi il tasto **Browse** ed indicare la path contenente il firmware decompresso. E' inoltre opportuno scegliere se mantenere gli attuali settaggi (**Current Settings**) o ripristinare il dispositivo alle condizioni iniziali (**Factory Default Settings**).
Premere poi sul tasto **Upgrade** per terminare l'aggiornamento.



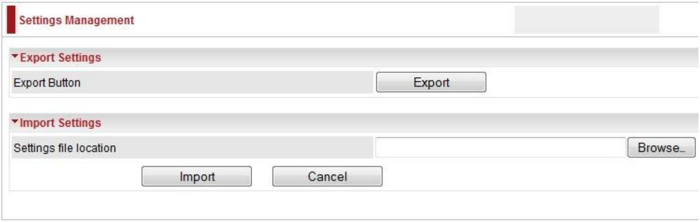
- E' opportuno garantire, durante l'intera fase di upgrade, al dispositivo l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.
- Effettuare l'upgrade utilizzando una connessione wired e non wireless. Questo potrebbe danneggiare il dispositivo ed invalidare così la garanzia.
- Non utilizzare file di restore generati con versioni anteriori di firmware. Questo potrebbe rendere instabile il dispositivo.
- Durante la procedura di upgrade è opportuno non chiudere il browser Web, caricare nuove pagine o cliccare su link. Questo potrebbe danneggiare il firmware e rendere inusabile il dispositivo.

Durante la fase di upgrade il dispositivo indicherà lo stato di completamento della riscrittura del firmware mostrando un indicatore percentuale (sotto riportata). Il processo terminerà col riavvio del dispositivo.


Atlantis
Net Fly AP3WN
Status
LAN Setting
Wireless Settings
Administration
Management
Firmware Upgrade
Settings Management
Restart
Firmware Upgrade Progress
Upload firmware completed, system is rebooting, please wait a minute...
Progress :
Please wait 2 second for system reboot complete.
After system reboot complete, the browser will redirect to to http://192.168.1.252/home.asp

9.12 Administration -> Settings Management

NetFly AP3 WN consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.



Per effettuare il Backup cliccare sul bottone **Export**. Non resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file con estensione DAT).
Per effettuare il Ripristino cliccare sul bottone **Browse**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su **Import.**
La procedura è piuttosto lenta (il tempo complessivo può superare i 2 minuti) e termina con il riavvio del dispositivo.



Non editare per nessuna ragione il file di backup, questo potrebbe bloccare e rendere inutilizzabile il dispositivo.
I file DAT di ripristino vanno utilizzati su apparati con la medesima release di firmware da cui sono stati generati.

9.13 Administration -> Restart

Se per necessità si desidera reimpostare il NetFly AP3 WN con la configurazione di default (perdendo tutti i settaggi inseriti) è sufficiente accedere, sotto il menù **Administration -> Restart** alla voce **Restart** e spuntare la voce **Factory default settings**. Premere poi il tasto **Restart.** Il dipositivo effettuerà un reboot e caricherà i settaggi di default.



Premendo invece il tasto **Restart** con la scelta **Current Settings** il dispositivo effettuerà un reboot caricando la configurazione attuale.

10. Supporto

Per qualunque altro problema o dubbio sul funzionamento del prodotto, è possibile contattare il servizio di assistenza tecnica Atlantis tramite l'apertura di un ticket on-line sul portale http://www.atlantis-land.com/ita/supporto.php. Nel caso non fosse possibile l'accesso al portale di supporto, è altresì possibile richiedere assistenza telefonica al numero 02/ 78.62.64.37 (consultare il sito per verificare gli orari in cui il servizio viene erogato).

Per esporre eventuali richieste di supporto prevendita o richieste di contatto , si invita ad utilizzare gli indirizzi mail info@atlantis-land.com oppure prevendite@atlantis-land.com.

Atlantis SpA
Via S. Antonio, 8/10
20020 Lainate (MI)
Fax: +39.02.78.62.64.39
Website: http://www.atlantis-land.com
Email: info@atlantis-land.com

APPENDICE A: Troubleshooting

Questo capitolo illustra come identificare e risolvere eventuali problemi sul NetFly AP3 WN.

A.1 Utilizzare i LED per la diagnosi dei problemi

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED PWR non si accende

Steps	Azione Correttiva
1	Accertarsi che la presa elettrica cui lapparato è collegato eroghi tensione.
2	Controllare che il meccanisco di inserzione della presa sia correttamente bloccato (si faccia riferimento alla sezione 3 di questo manuale).
4	Se il problema persiste contattare l'assistenza tecnica Atlantis.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra il NetFly e il PC o lo Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis.

A.2 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, è necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante "Reset" presente nel pannello posteriore del prodotto per 3 (o più) secondi, il router riporterà tutte le impostazioni ai valori iniziali.

2	I parametri di default per l'accesso alla configurazione del Router ADSL sono: Indirizzo IP:192.168.1.252 Username: admin Password: atlantis
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.3 Interfaccia LAN

Le schermate di configurazione Web non vengono visualizzate correttamente.

Steps	Azione correttiva
1	Accertarsi di utilizzare Internet Explorer 5 o una versione successiva.
2	Eliminare i files temporanei di Internet ed eseguire un nuovo login.

Non è possible accedere ad Internet, benché accedo al NetFly AP3 WN.

Steps	Azione correttiva
1	Il dispositivo integra un server DHCP, per facilitarne la configurazione. Questo server andrebbe disabilitato se sulla rete è presente un altro apparato con server DHCP attivo (tipicamente il router ADSL). Verificare questo punto.

Non è possible accedere al NetFly AP3 WN tramite il servizio Telnet.

Steps	Azione correttiva
1	Il dispositivo non supporta tale modalità di configurazione.

A.4 Interfaccia WLAN

Come faccio ad aumentare la portata dell'apparato?

Steps	Azione correttiva
1	Verificare che non siano presenti altre reti Wireless con canali in sovrapposizione**.** Accedere al menù **Wireless Settings->Basics**. Impostare la combo-box **Channel ID** su **Auto** e cliccare su **Apply.**
2	Passare alla modalità **Advanced.** Accedere al menù **Wireless Settings->Advanced**. Verificare, solo se la modulazione scelta è **IEE802.11g**, che il valore del campo **Tx PowerLevel** sia **100. Consultare eventuali aggiornamenti di questa FAQ sul sito prima di cambiare questo valore.**
3	Aggiornare i driver dei client utilizzati.

4	Valutare l'ipotesi di utilizzare la funzionalità WDS per estendere la portata (si consulti il manuale per ulteriori dettagli).

A.5 Wireless

Domanda	Risposta
Posso avviare un' applicazione da un computer remoto presente sulla rete wireless?	Questo dipende direttamente dall'applicazione stessa, se è stata progettata per lavorare in rete (non fa differenza che sia wireless o cablata) non ci sarà alcun problema.

Steps	Risposta
Posso giocare in rete con gli altri computer presenti sulla WLAN?	Si, se il gioco è dotato di funzionalità multiplayer in rete.

Steps	Risposta
Cos'è lo Spread Spectrum?	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.

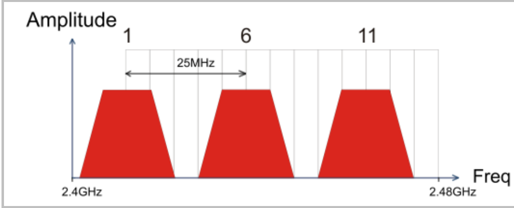
Steps	Risposta
Cosa sono DSSS e FHHS?	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHHS (Frequency Hopping Spread Spectrum): è una tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.

<table>
<tr><th>Steps</th><th>Risposta</th></tr>
<tr><td>Cos’è un decibel?</td><td>Il deciBel è un’unita misura relativa che esprime un rapporto fra 2 valori. E’ importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E’ utilizzato perché permette di avere un’immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare.
L’equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.</td></tr>
<tr><td>dBm</td><td>Definiamo il dBm=10 log 10 (P 2 / P 1), dove P1 =1 milliWatt (mW).
E’ possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm.
Nella tabella seguente è riportata l’equivalenza per i valori più comuni (utilizzare la formula di sopra per valori non in tabella):
<table>
<tr><td>dBm</td><td>Watt</td><td>note</td></tr>
<tr><td>0</td><td>1 mW</td><td></td></tr>
<tr><td>3</td><td>2 mW</td><td></td></tr>
<tr><td>6</td><td>4 mW</td><td></td></tr>
<tr><td>9</td><td>8 mW</td><td></td></tr>
<tr><td>10</td><td>10 mW</td><td></td></tr>
<tr><td>12</td><td>15,8 mW</td><td></td></tr>
<tr><td>13</td><td>20 mW</td><td></td></tr>
<tr><td>14</td><td>25 mW</td><td></td></tr>
<tr><td>15</td><td>32 mW</td><td></td></tr>
<tr><td>16</td><td>40 mW</td><td></td></tr>
<tr><td>17</td><td>50 mW</td><td></td></tr>
<tr><td>18</td><td>63 mW</td><td></td></tr>
<tr><td>19</td><td>79 mW</td><td></td></tr>
<tr><td>20</td><td>100 mW</td><td>Massima Potenza utilizzabile per WLAN a 2.4Ghz</td></tr>
<tr><td>23</td><td>200 mW</td><td></td></tr>
<tr><td>26</td><td>400 mW</td><td></td></tr>
<tr><td>29</td><td>800 mW</td><td></td></tr>
</table></td></tr>
<tr><td>dBi</td><td>Il guadagno di un'antenna è definito come il rapporto fra la</td></tr>
</table>

	densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P 2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza. Definiamo il dBi=10 log 10 (P 2 / P isotropica), dBm=10 log 10 (Potenza/ 1mW)
Antenna Isotropica	Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare. L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.
Antenna Direttiva	Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza.

Interferenze sulla WLAN?

Steps	Risposta
Banda ISM	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.
Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?	Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze. Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi. In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.
Canali	Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente

	soltanto 3 dei 13 canali disponibili. E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6). L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**". Il disegno seguente illustra meglio quanto detto:  Sino a 3 AP possono coesistere senza overlapping. E' opportuno prestare attenzione all'assegnazione dei canali.

Domande Varie ?

Steps	**Risposta**
WDS	Il WDS (Wireless Distribution System) è la tecnologia che permette ad un Access Point di svolgere contemporanemente la funzionalità di AP e di Repeater del segnale. Risulta essere la soluzione ottimale per estendere la copertura di una wireless LAN in ambienti dove non è assolutamente possibile stendere cavi. Può essere utile per raggiunge relocazioni remote. Va osservato che l'uso di un repeater ha un forte impatto sulle prestazioni dei client wireless ad esso collegati. Apparati che supportano tale tecnologia, a listino Atlantis land sono: A02-AP1-W54 A02-AP1-W54PoE A02-RA242-W54
IEEE802.11g	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e

	quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.
Infrastructure	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point.
Sicurezza	L'Access Point offre funzionalità di crittografia WEP fino a 128 bit, ciò provvede a rendere sicure le trasmissioni dati wireless. L'utilizzo del WPA e/o WPA2 rende ancora più sicura la trasmissione wireless. Tali tecnologie devono essere supportate anche dai vari client utilizzati.

APPENDICE B: WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) è un insieme di specifiche mirate a facilitare notevolmente le operazioni di aggiunta di dispositivi alla propria rete wireless e la messa in sicurezza della stessa con la sola pressione di un pulsante oppure tramite l'immissione di un codice PIN.
I dispositivi conformi alle specifiche WPS sono quindi in grado, in maniera molto semplice, di rilevare le reti con tale supporto, acquisirne le impostazioni basilari(quali SSID e canale) e negoziare in maniera del tutto automatica un profilo di sicurezza utiizzando i più avanzati algoritmi di crittografia come WPA e WPA2.
Nella configurazione PIN, un codice PIN univoco viene assegnato ad ogni dispositivo che deve far parte della rete; un adesivo o un etichetta posta sulla parte posteriore del client identificheranno tale codice in caso di PIN statico, o in alternativa questo verrà generato in maniera dinamica e visualizzato tramite utility.
Questo codice viene utilizzato per assicurare l'identificazione univoca della periferica e per evitare intrusioni all'interno della rete da parte di periferiche esterne. Gli utenti, per poter aggiungere il dispositivo alla rete, dovranno inserire all'interno del Registar (presente all'interno dell'Access Point), il codice PIN identificativo della periferica da connettere.
Nella configurazione PCB, l'utente sarà in grado di aggiungere periferiche e mettere in sicurezza la propria rete tramite la semplice pressione di un pulsante (fisico sugli Access Point e virtuale sui dispositivi client).
Di seguito una tabella riassuntiva sui vantaggi del supporto WPS e sulle modalità di configurazione:

Senza WPS	Con WPS (PIN mode)	Con WPS (PCB mode)
Accensione dell'Acces Point	Accensione dell'Acces Point	Accensione dell'Acces Point
Accesso all'Access Point	Attivazione del client	Attivazione del client
Configurazione dell'SSID	Generazione in maniera automatica dell'SSID e broadcasting della stessa.	Generazione in maniera automatica dell'SSID e broadcasting della stessa.
Attivazione della sicurezza	Accesso al Registar presente sull'Access Point	Pressione del bottone sull'Access Point e sul client
Impostazione della parola di accesso (WPA) o delle chiavi di accesso (WEP)	Insierimento del PIN relativo al client da aggiungere.	
Attivazione del client	Avvio della	

	sincronizzazione tra AP e client	
Selezione della rete a cui connettersi		
Inserimento della chiave di sicurezza per la connessione del client		

APPENDICE C: Connessione usando il Client di Windows

In Windows XP/Vista e 7 è incluso un client che permette la gestione di un adattatore wireless al pari delle Utility.

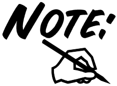
Windows 7

- Cliccare sull'icona di rete posizionata sulla System Tray (vedi immagine) e selezionare l'opzione **Centro connessioni di rete e condivisione** oppure cliccare su **Start -> Pannello di Controllo -> Centro connessioni di rete e condivisione**.



- Selezionare l'opzione **Connessione a una rete** dal menu di sinistra per visualizzare la lista di reti wireless disponibili.
- Selezionare l'SSID della rete **A02-AP3-W300N** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPAPSK,** Encrypton: **AES**, Encryption Key: **NetFlyAP3WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB/PCI all'AP.



Nel caso in cui non sia possibile visualizzare la lista di reti senza fili disponibili, si prega di verificare la corretta installazione dei driver del client USB/PCI.

Windows VISTA

- Cliccare sull'icona di rete posizionata sulla System Tray (vedi immagine) e selezionare l'opzione **Centro connessioni di rete e condivisione** oppure cliccare su **Start -> Pannello di Controllo -> Centro connessioni di rete e condivisione**.



- Selezionare l'opzione **Connessione a una rete** dal menu di sinistra per visualizzare la lista di reti wireless disponibili.
- Selezionare l'SSID della rete **A02-AP3-W300N** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPAPSK,** Encrypton: **AES**, Encryption Key: **NetFlyAP3WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB/PCI all'AP.

NOTE: Nel caso in cui non sia possibile visualizzare la lista di reti senza fili disponibili, si prega di verificare la corretta installazione dei driver del client USB/PCI.

Windows XP

- Fare doppio click sull'icona di rete posizionata sulla System Tray (vedi immagine).



- Selezionare l'SSID della rete **A02-AP3-W300N** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPAPSK,** Encrypton: **AES**, Encryption Key: **NetFlyAP3WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB/PCI all'AP.

NOTE:

Nel caso in cui non sia possibile visualizzare la lista di reti senza fili disponibili, si prega di verificare l'avvio del servizio **Zero Configuration** (vedi appendice A) e la corretta installazione dei driver del client USB/PCI.

NOTE:

Di seguito è indicato come disabilitare il servizio Zero Configuration di Windows XP, al fine di poter controllare il dispositivo tramite l'utility fornita a corredo:

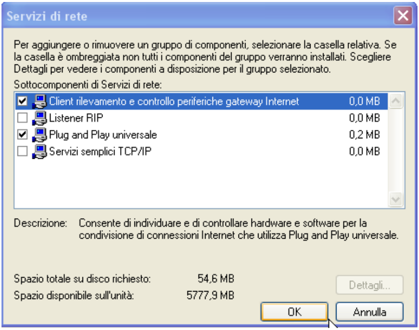
- Cliccare su **Start** e poi su **Pannello di Controllo**
- Selezionare dal menu di sinistra la voce **Visualizzazione classica**
- Cliccare su **Strumenti di amministrazione**
- Cliccare su **Servizi**
- Selezionare il servizio **Zero Configuration** e cliccare su **Proprietà**
- Cliccare sul pulsante **Arresta** per terminare temporaneamente il servizio
- Impostare il campo **Tipo di Avvio** su **Disabilitato** come da figura

APPENDICE D: Universal Plug'n'Play (UPnP)

Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di autoconfigurarsi senza l'intervento dell'utente. Chiunque dunque sarà in grado, senza conoscere complicati concetti, di godere pienamente dei vantaggi del NAT e contemporaneamente utilizzare le più comuni applicazioni Internet senza il minimo problema.

Attivazione dell'UPnP in Windows XP.

Pannello di Controllo poi **Installa applicazioni**, scegliere **Installazione Componenti di Windows**. Selezionare **Servizi di Rete** e poi cliccare su **Dettagli.** Assicurarsi che siano spuntate le seguenti voci: Plug and Play Universale e Client rilevamento e controllo periferiche Gateway Internet.



Andando su **Risorse di Rete** è possibile trovare il nome del campo **Set Host Name.** Cliccandoci sopra è possibile entrare nella configurazione del WebShare Wireless ADSL2+ Router . Cliccando il tasto destro e poi Proprietà è possibile avere accesso ad informazioni supplementari.

Andando su Pannello di Controllo e poi Connessioni di rete è possibile cliccare sull'icona Connessione Internet.



Scegliendo proprietà e poi impostazioni è possibile impostare le configurazioni necessarie all'uso dell'UPnP. Basterà premere aggiungi per creare una sorta di Virtual Server per l'applicazione del caso.



- **Descrizione del Servizio**: identificativo
- **Nome o Indirizzo IP**: IP del PC su cui risiede il server
- **Numero di porta esterna del servizio**: immettere la porta esterna (es 80 per http, 20-21 per FTP)
- **Numero di porta interna del servizio**: immettere la porta interna

- Scegliere il protocollo tra **UDP** o **TCP**.

Premendo **OK** il protocollo UPnP dialogherà col WebShare 141W Modem/Router .

In questa modalità è possibile configurare una sorta di Virtual Server da ogni PC senza accedere al WebShare 141W vero e proprio.
Alcune applicazioni sono in grado di configurare in maniera autonoma il servizio UPnP.

NOTE: E’ necessario attivare l’UPnP del dispositivo accedendo alla sezione Advanced Setup, poi UpnP. Qui è possibile attivare il servizio e/o concedere alle applicazioni compatibili la possibilità di configurazione automatica del router.

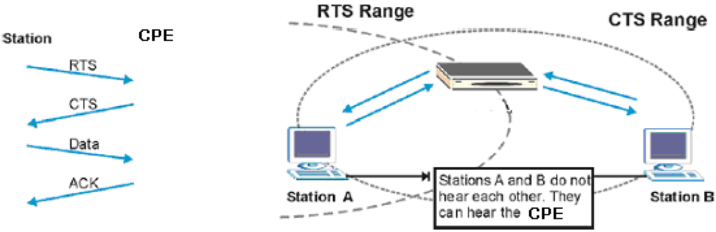
APPENDICE E: Rete Wireless

Introduzione alla rete Wireless
Questa sezione presenta la Wireless Lan e alcune configurazioni di base. Una Wireless Lan può essere creata semplicemente con due computer dotati di schede di rete Wireless che comunicano in una rete di peer-to-peer oppure in maniera più complessa utilizzando più computers con schede di rete senza fili che comunicano attraverso punti di accesso che fanno da ponte tra la rete Wireless e la rete cablata.

Canali
Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).

ESS ID
L' Extended Service Set (ESS) consiste in un gruppo di Access Point o Gateway Wireless connessi ad un LAN cablata sulla stessa subnet. Un ESS ID identifica univocamente ogni gruppo. Ciascun Access Point o Gateway Wireless e le stazioni Wireless a loro associate devono avere lo stesso ESSID.

RTS/CTS
Quando due stazioni Wireless sono all'interno del range dello stesso Access Point ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.

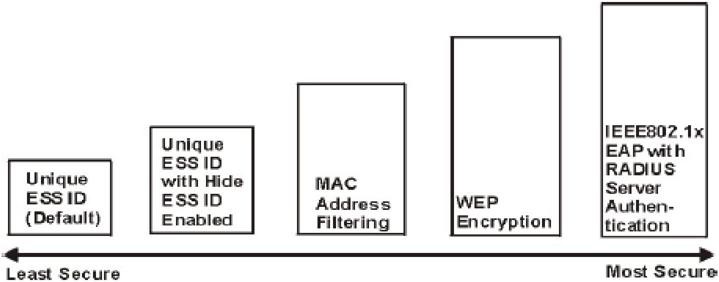


La stazione A invia dei dati al Router ADSL ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono all'Access Point.
Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS all' Access Point per ottenere il permesso ad iniziare. L'Access Point invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.

Fragmentation Threshold (Soglia di frammentazione)
Il Fragmentation Threshold è la dimensione massima di frammentazione dei dati (tra 256 e 2432 bytes) che può essere trasmessa in una rete Wireless prima che il Router ADSL effettui un ulteriore divisione in frames più piccoli.
Un alto valore di Fragmentation Threshold è indicato per reti esenti da interferenze, mentre per reti soggette ad interferenze e con un traffico molto elevato è preferibile optare per un valore più basso.
Se viene impostato un valore più basso dell'RTS/CTS i dati verranno frammentati prima della fase di handshake la quale non verrà effettuata.

Livello di Sicurezza
Le funzionalità di Wireless Security sono necessarie per proteggere le comunicazione tra stazioni Wireless , Access Point e la rete cablata.

La figura sotto indica i possibili livelli di sicurezza Wireless firniti dal Router ADSL. Il livello di sicurezza più alto conta sul protocollo EAP (Extensible Authentication Protocol) per l'autenticazione ed utilizza WEP con scambio di chiavi dinamico. Questo sistema richiede l'interazione con un server RADIUS (Remote Authentication Dial-In User Service) che offre servizi di autenticazione per stazioni Wireless.



Se none viene utilizzato alcuna funzionalità di Wireless Security il Router ADSL sara accessibile da qualsiasi stazione Wireless presente nel suo campo di azione. E' possibile configurare questo servizio tramite l'interfaccia di configurazione Web del prodotto.

Cifratura dati con WEP
La cifratura WEP provvede al crittaggio dei dati trasmessi sulla rete in modo da ottenere una comunicazione privata. Il crittaggio viene effettuato sia su comunicazioni unicast che multicast.
Tutte le stazioni Wireless che utilizzano questa cifratura devono utilizzare la stessa chiave per la cifratura e la decodifica dei dati. Il Wireless Router ADSL2+ è in grado di utilizzare chiavi di criptaggio da 64 e 128 bit.

APPENDICE F: Copertura

Considerazioni Generali

In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire diverse decine di metri. E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine.

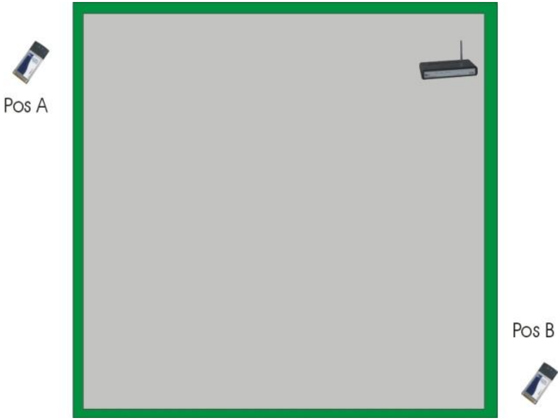
Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.

- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E' bene prendere in considerazione questo fatto.

- Allontanare l'AP Wireless da ogni altro dispositivo che produca emissioni RF.

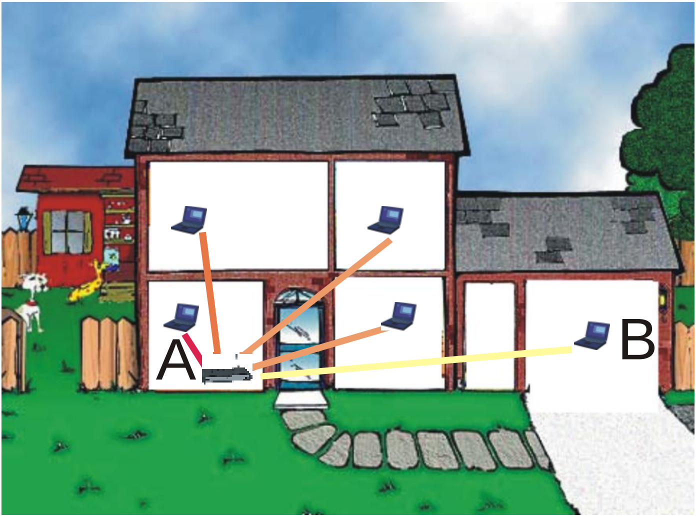
- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless AP col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante). Si veda la figura sottostante:



Il Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A, benché la distanza effettiva dall'AP sia quasi identica nei 2 casi. E' sufficiente collocare il Wireless AP al centro del locale per migliorare decisamente le prestazione del client B.

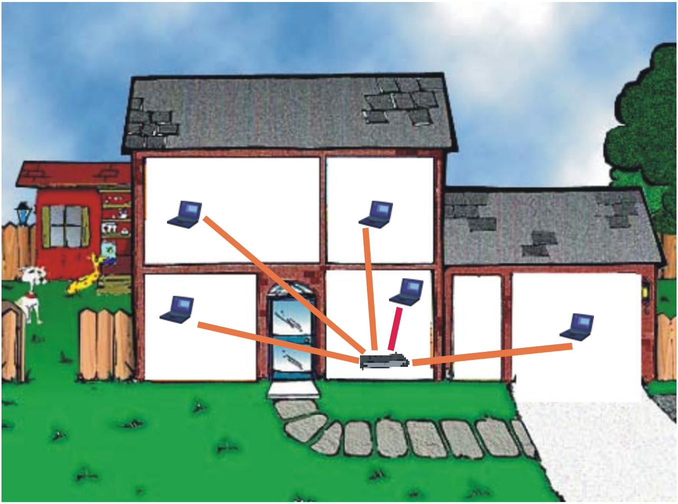
Dove installare un AP

Immaginiamo di avere un'installazione come quella in figura.



Sicuramente Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A.

E’ sufficiente collocare il Wireless Router/AP al centro della rete per migliorare decisamente le prestazione di entrambi i client B.



Si è operato sulla diminuzione 2 fattori:

- Distanza media
- Sezioni di muro attraversate

E' decisamente meglio avere una rete i cui client abbiano un link mediamente buono che non una rete con taluni client con link eccellente ed altri con link molto scarso.

La stazione lontana, che generalmente trasmette con un data rate più basso, tende a consumare un «airtime» elevato.

L'AP ha meno tempo da dedicare a client più vicini e più veloci.

Prestazioni complessivi peggiori.

APPENDICE G: LISTA CANALI

Determinati paesi appartenenti alla CE possono avere regolamentazioni particolari. L'utente deve conoscere queste peculiarità e scegliere, utilizzando la tabella seguente, in base al paese dove l'apparato è utilizzato i canali permessi.

Country Name	Classification	Range
Argentina, Bahrain, Brazil, Canada, Chile, Croatia, Ecuador, Hong Kong, Malaysia, Mexico, Panama , Peru, Philippines, Puerto Rico, Romania, Saudi Arabia, Taiwan, Unite States of America, Uruguay, Venezuela, Yugoslavia	0	CH1~11
Australia, Austria, Belarus, Belgium, Bolivia, Bulgaria, China, Colombia, Costa Rica, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan3, Jordan, Kuwait, Latvia, Lebanon, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Macedonia, Morocco, Netherlands, New Zealand, Nigeria, Norway, Paraguay, Poland, Portugal, Russia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Turkey, United Arab Emirates, United Kingdom	1	CH1~13
France2	3	CH10~13
Japan	5	CH1~14
Japan2	4	CH14~14

APPENDICE H: Caratteristiche Tecniche

Technical Specs	
Product Code	A02-AP3-W300N
Standards	IEEE 802.11b/g/n
Chipset	RaLink® RT3052 (MIPS 24KEc 384MHz with 32KB I-cache/16KB D cache)
Interface	1 x Fast Ethernet (LAN)
LED	3 (LAN, WLAN, Power)
WPS/Reset	Yes/Yes
Antenna	2 x 2 dBi fixed external Antennas
Virtual AP	• VLAN tagging • Client Isolation • Multiple SSID Isolation
Multiple SSID	• Up to 4 SSID (each SSID uses different encryption key) • Multiple SSIDs allow users to access different networks through a single access point (all, only LAN, only WAN)
WDS	With WDS (Wireless Distribution System) mode, user can use wireless media to communicate two or more LANs through the AP with WDS mode, all of the LAN will be combined in the WDS group. The WDS feature (up to 4 AP) makes the device an ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, or even at hotspots.
Advanced Features	• Wireless Client Mode (WDS Bridge Mode) • DHCP Server • WMM • IGMP • UPnP
Frequency Band	2412 ~ 2472MHz
Radio Technology	• IEEE 802.11g/n: Orthogonal Frequency Division Multiplexing (OFDM) • IEEE 802.11b: Direct Sequence Spread Spectrum (DSSS)
Modulations Scheme	DBPSK/DQPSK/CCK/OFDM
Media Access Protocol	CSMA/CA with ACK
Transmission Rate	Up to 300Mbps (auto-sense with auto fallback)

Wireless Security	• 64/128-bit WEP, WPA-PSK, WPA2-PSK • WPA, WPA2 with Radius • MAC Access Control List • WPS™
Transmitting Power	802.11b/g/n: up to 16 ± 1 dBm
Receiver Sensitivity	• 802.11b (1Mbps): -90dBm @8% PER • 802.11b (6Mbps): -88dBm @8% PER • 802.11b (11Mbps): -85dBm @8% PER • 802.11g (54Mbps): -68dBm @10% PER • 802.11n (135Mbps): -68dBm @10% PER • 802.11n (270Mbps): -68dBm @10% PER • 802.11n (300Mbps): -68dBm @10% PER
Number of Operational Channel	Europe (13)
Range Coverage	• Indoor: up to 120 meters • Outdoor: up to 350 meters
Certifications	CE (Europe)
Dimensions (mm)/ Weight	110mm x 80mm x 35mm (without Antenna and plug) / 220g
Temperature Range	Operation: 0°C ~ 32°C Storage: -10°C ~ 60°C
Humidity	10% ~ 75% (non Condensing)
System Requirements	• TCP/IP protocol must be installed on each PC • Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
Package Contents	• One NetFly AP3 N • 1 x RJ45 CAT5 Cable • Quick Start Guide (English and Italian) • CD-Rom with QSG and Manual (English and Italian) • 1 x Warranty Card and 1 x WEEE Card

Specifications are subjected to change without prior notice. No liability for technical errors and/or omissions
Performance and Throughput are influenced by many factors (interference, noise, environments)

Atlantis

Atlantis SpA
Via S. Antonio, 8/10
20020 Lainate (MI)
info@atlantis-land.com